

UNITED STATES DISTRICT COURT

for the
Northern District of California

FILED

Jul 09 2024

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
APPLICATION BY UNITED STATES FOR SEARCH
WARRANT FOR ONE EMAIL ACCOUNT FOR
INVESTIGATION OF 18 U.S.C. § 1347

Case No. 4:24-mj-71033-KAW

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1347	Healthcare fraud
18 U.S.C. §§ 371, 1349, 286	Conspiracy to commit healthcare fraud and defraud the United States
18 U.S.C. § 287	Submission of false, fictitious or fraudulent claims to the United States

The application is based on these facts:

See Attached Affidavit of U.S. Department of Health & Human Services Office of Inspector General Special Agent (HHS-OIG) Jin Tae Kim

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Approved as to Form:

Benjamin K. Kleinman
AUSA BENJAMIN K. KLEINMAN

Jin Tae Kim /s/
Applicant's signature

JIN TAE KIM, Special Agent - HHS-OIG
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: July 9, 2024

City and state: Oakland, CA

Kandis Westmore
Judge's signature

Hon. Kandis A. Westmore, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Jin Tae Kim, a Special Agent of the Department of Health and Human Services, Office of Inspector General, Office of Investigations (“HHS-OIG”), being duly sworn, hereby declare as follows:

OVERVIEW AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with MICROSOFT SharePoint and Teams chats, videos, and messages, (the “**Applications and Services**”) accounts associated with the domain vbshealthcare.com and https://vbshealthcare-my.sharepoint.com (the “**Subject Accounts**”) that are stored at premises controlled by MICROSOFT an electronic communications service provider and remote computing service headquartered at 1 Microsoft Way, Redmond, Washington 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MICROSOFT to disclose to the government copies of the information (including the content of communications) further described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, government-authorized persons will review that information to locate the items described in Section III of Attachment B.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Virtual Benefit Solutions Inc, Hearing Clinic “VBS”¹ and Tyrone Moore (“MOORE”) have violated 18 U.S.C. § 1343 (wire fraud), 1347 (healthcare fraud), 371, 1349, 286 (conspiracy to commit healthcare fraud and defraud the United States), 287 (submission of false, fictitious or fraudulent claims to the United States), and 1957 (engaging in monetary transactions in property derived from specified unlawful activity)

¹ Virtual Benefits Solutions Incorporated, Hearing Clinic “VBS” has also been known to go by the names Virtual Hearing Clinic “VHS” and Virtual Benefits Solutions Incorporated - Health & Wellness or simply Virtual Benefits Solutions. The names are used interchangeable by witnesses and in this affidavit.

(“**SUBJECT OFFENSES**”). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

3. The facts in this affidavit come from my personal observations, my training and experience, information from records and databases, and information obtained from other law enforcement agents (“Federal Agents”) and witnesses. This affidavit does not set forth all of my knowledge about this matter; it is intended to only show that there is sufficient probable cause for the requested warrant.

AFFIANT BACKGROUND

4. I am a Special Agent with HHS-OIG assigned to investigate possible violations of federal criminal law, specifically investigations involving health care fraud, and have been so employed since September 2018. I have received specialized training in health care fraud matters including, but not limited to, Anti-Kickback, Mail Fraud, Wire Fraud, and False Claims. As an HHS-OIG agent, I am authorized to investigate violations of United States law and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. Prior to my current position as a Special Agent with HHS-OIG, I was a Postal Inspector with the United States Postal Inspection Service for approximately 3 years.

5. I am working with the Federal Bureau of Investigation (“FBI”) Special Agent James Gawrych and Internal Revenue Service, Criminal Investigation (“IRS-CI”) Special Agent Kendl Tovey in the investigations described below. The facts set forth in this affidavit are based upon my personal observations, my training and experience, documents and records that were collected and reviewed in the course of this investigation by myself and other agents, and information provided by witnesses. This affidavit is intended only to show that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter.

APPLICABLE STATUTES

6. 18 U.S.C. § 1343 (wire fraud), 1347 (healthcare fraud), 371, 1349, 286 (conspiracy to commit healthcare fraud and defraud the United States), 287 (submission of false, fictitious or fraudulent claims to the United States).

7. 18 U.S.C. §§ 1956 and 1957 criminalize various activities that constitute money laundering. These activities include but are not limited to conducting financial transactions with knowledge that the proceeds involved in the financial transaction are proceeds from a “specified unlawful activity” and with the intent to “promote the carrying on of a specified unlawful activity,” see 18 U.S.C. § 1956(a)(1)(A); or knowing that the transaction is designed in whole or in part to “conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or to avoid a transaction reporting requirement under State or Federal law.” See 18 U.S.C. § 1956(a)(1)(B)(i) & (ii). Additionally, it is a crime to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from a specified unlawful activity. See 18 U.S.C. §1957.

8. Furthermore, it is a crime to conduct or attempt to conduct a financial transaction involving property represented to be the proceeds of a specified unlawful activity with the intent to promote the carrying on of a specified unlawful activity; conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity; or avoid a transaction reporting requirement under State or Federal law. The term “represented” means any representation made by a law enforcement officer or by another person at the direction of, or with the approval of, a Federal official authorized to investigate or prosecute violations of this section. See 18 U.S.C. § 1956(a)(3).

9. Under 18 U.S.C. § 1956, a “financial transaction” includes a transaction which affects interstate or foreign commerce and involves the movement of funds by wire or other means. Furthermore, a “monetary transaction” includes the transfer or exchange in or affecting interstate or foreign commerce of funds by, through, or to a financial institution. “Specified

unlawful activities” include violations of 18 U.S.C. § 1343. See 18 U.S.C. § 1956(c)(7)(A).

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

11. Under 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

INFORMATION ABOUT MICROSOFT

12. According to the MICROSOFT website, SharePoint can be used to create websites and also be used as a secure place to store, share, organize, and access information from any device with access to a web browser. SharePoint allows a business to create sites that employees can use to share documents and information with each other and with individuals outside the organization. An example of a SharePoint link is <https://vhshealthcare-my.sharepoint.com> listed in Attachment A.

13. According to the MICROSOFT website, Teams is used for instant messaging, audio and video calling, files and data collaboration for companies. From my experience, a Teams account is often associated with a similar domain as a company’s Outlook domain listed in Attachment A.

14. Outlook allows subscribers to obtain email accounts at the domain name outlook.com. The email ending in domain vbshealthcare.com is hosted by Microsoft Outlook and listed in Attachment A. VBS has used SharePoint, Teams, and Outlook as part of their business operations.

15. In my training and experience, I have learned that MICROSOFT provides a variety of online services, **Applications and Services**, to the public. MICROSOFT allows subscribers to obtain **Applications and Services** accounts. The **Applications and Services** account information listed in Attachment A, is hosted by MICROSOFT. Subscribers obtain an

account by registering with MICROSOFT. During the registration process, MICROSOFT asks subscribers to provide basic personal information. Therefore, the computers of MICROSOFT are likely to contain stored electronic communications (including retrieved and unretrieved email for MICROSOFT subscribers) and information concerning subscribers and their use of MICROSOFT services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. A MICROSOFT subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by MICROSOFT. In my training and experience, evidence of who was using an **Applications and Services** account may be found in address books, contact or buddy lists, email in the account, and shared links containing file access, including pictures and files.

17. In my training and experience, **Applications and Services** providers generally ask their subscribers to provide certain personal identifying information when registering for an account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

18. In my training and experience, **Applications and Services** providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the

status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

19. In my training and experience, in some cases, **Applications and Services** users will communicate directly with the provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. Information stored in connection with a **Applications and Services** account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an **Applications and Services** account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, files and images links sent may indicate who used or controlled the account at a relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, **Applications and Services** providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with

the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner.

Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

THE MEDICARE PROGRAM

21. The Medicare Program ("Medicare") is a federally funded program that provides free and below-cost health care benefits to people age 65 years or older, the blind, and the disabled. The Centers for Medicare & Medicaid Services ("CMS") is responsible for the administration of the Medicare Program.

22. Individuals who receive benefits under Medicare are referred to as Medicare "beneficiaries." Beneficiaries are eligible to receive a variety of services, including hospital services ("Part A"), physician services ("Part B"), and prescription drug coverage ("Part D"). Medicare Advantage, formerly known as Part C, consists of private health insurance plans that were required to provide Medicare beneficiaries with the same services and supplies offered under Medicare Parts A and B. Part B covers outpatient physician services, such as office visits, minor surgical procedures, and laboratory services, such as drug testing and genetic testing, when certain criteria are met.

23. Providers ("Providers") include clinical laboratories, physicians, and other health care providers who provide services to beneficiaries. To bill Medicare, a provider must submit an enrollment application to Medicare. The enrollment application contains certification statements that the provider must agree to before enrolling with Medicare. Specifically, the certification

statement sets forth, in part, that the provider agrees to abide by the Medicare laws, regulations, program instructions, and will not knowingly present or cause to be presented a false or fraudulent claim for payment by Medicare.

24. A Medicare “provider number” is assigned to a provider upon approval of the Provider’s Medicare application. A Provider may use that provider number to file claims with, or “bill” Medicare to obtain reimbursement for services rendered to beneficiaries. When submitting claims to Medicare for reimbursement, Providers certify that: (1) the contents of the forms are true, correct, and complete; (2) the forms are prepared in compliance with the laws and regulations governing Medicare; and (3) the services purportedly provided, as set forth in the claims, are medically necessary.

BACKGROUND REGARDING COVID-19 UNINSURED PROGRAM

25. Since March 2020, several legislative acts designed to provide financial assistance and reimbursements to health care providers treating uninsured individuals during the COVID-19 pandemic have been passed by Congress and signed in to law.

26. In March 2020, the Families First Coronavirus Response Act (“FFCRA”) provided \$1 billion to the Public Health and Social Services Emergency Fund (“PHSSEF”), to be administered by the U.S. Department of Health and Human Services (“HHS”), for reimbursement to hospitals and other health care Providers for COVID-19 related treatment and services or visits of uninsured individuals through the Uninsured Program (“UIP”).

27. The FFCRA defines an uninsured individual as someone who is not enrolled in: A) a Federal health care program (e.g., Medicare or Medicaid), including an individual who is eligible for medical assistance by reason of and during any portion of the emergency period; (B) a group health plan or health insurance coverage offered by a health insurance issuer in the group or individual market; or (C) the Federal Employees Health Benefits Program.

28. The Health Resources and Services Administration (“HRSA”), an agency of HHS, oversees and administers these funds through the COVID-19 Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the

Uninsured Program (“the HRSA Program”). To participate in the HRSA Program, an individual authorized to attest on behalf of the Provider (the “recipient”) must attest to compliance with the Terms and Conditions for Participation in the HRSA Program (“HRSA Program Terms and Conditions”). Recipients must acknowledge that each time the recipient submits a claim for reimbursement for COVID-19 testing and/or testing-related items and services provided to individuals who did not have health coverage at the time the services were provided (“uninsured individuals”), each claim must be in full compliance with the HRSA Program Terms and Conditions.

29. The HRSA Program Terms and Conditions define COVID-19 Testing as an in vitro diagnostic test for the detection of SARS-COV-2 or the diagnosis of the virus that causes COVID-19, and the administration of such test, that meets certain requirements, such as being approved or cleared by the FDA or authorized by the FDA for emergency use.

30. Recipients who attest to the HRSA Program Terms and Conditions make certifications that include, but are not limited to:

- a. The recipient or its agents provided the items and services on the claim form to the uninsured individuals identified, on or after February 4, 2020, and that all items and services for which payment is sought were medically necessary.
- b. To the best of the recipient’s knowledge, the patients identified on the claim form were uninsured individuals at the time the service was provided.
- c. The recipient will not use the payment from HRSA to reimburse expenses or losses that have been reimbursed from other sources or that other sources are obligated to reimburse.
- d. The recipient will not engage in “balance billing” or charge any type of cost sharing for any items or services provided to uninsured individuals receiving a COVID-19 testing and/or testing related items for which the recipient receives a payment from the HRSA Uninsured Program fund. The recipient “shall consider Payment received from the Uninsured Program Fund to be payment in full for such COVID-19 testing

and/or testing-related items...”

e. The recipient will maintain appropriate records and documentation required to substantiate payments. The recipient will promptly submit copies of such records and documentation upon request of appropriate regulators.

31. To claim reimbursement for COVID-19 testing of uninsured individuals, recipients must submit patient rosters to the HRSA Program web portal. If a patient’s social security number, state of residence, or state identification / driver’s license is not submitted, the recipient must attest that they attempted to capture this information before submitting a claim and the patient did not have this information at the time of service, or that the recipient did not have direct contact with the patient and thus did not have an opportunity to attempt to capture this information.

32. The UIP stopped accepting claims for testing and treatment on March 22, 2022, due to a lack of sufficient funds.

CLINICAL LABORATORY IMPROVEMENT AMENDMENT REGULATIONS

33. The Clinical Laboratory Improvement Amendments of 1988 (“CLIA”) is an amendment to the Public Health Services Act in which Congress revised the federal program for certification and oversight of clinical laboratory testing. See generally 42 U.S.C. § 263a. As a general matter, a laboratory is not permitted to solicit or accept specimens for testing unless CMS has issued it a certificate to do so. *Id.* at § 263a(b). CMS issued federal regulations titled “Standards and Certification: Laboratory Requirements” to enact CLIA.

34. In general terms, the CLIA regulations establish quality standards for laboratory testing performed on specimens from humans, such as blood, body fluid and tissue, for the purpose of diagnosis, prevention, or treatment of disease, or assessment of health.

35. Although CLIA is a federal program, State Agencies are responsible for laboratory oversight and maintaining CLIA laboratories certification of records. State Agencies process CLIA applications, renewals, updates, and requests for certificate copies.

36. CLIA defines waived tests as “simple laboratory examinations and procedures

that have an insignificant risk of an erroneous result.” The FDA determines which tests meet these criteria when it reviews manufacturer’s applications for test system waivers.

37. Waived tests are not exempt from CLIA. Facilities performing only those tests categorized as waived must apply for a CLIA certificate of waiver. Facilities must submit CMS-116 form requesting approval from CMS to conduct waived testing and other required documents to their respective state agencies who process the application. California Department of Public Health (“CDPH”) Division of Laboratory Field Services is the State Agency responsible for oversight and maintaining CLIA laboratories certification of records.

38. CLIA licenses are a federal certificate tied to a physical lab and is needed to conduct on-site testing. A different laboratory cannot use another lab’s CLIA license. A CLIA license is not needed if the lab is only collecting specimen and not performing any tests. To conduct COVID-19 testing in California, a lab would need either a federal CLIA license or CLIA waiver and a state license.

FACTS SUPPORTING PROBABLE CAUSE

39. VBS is incorporated in the State of California, with a listed address of 39899 Balentine Drive, Suite 200, Newark, California 94560, which is here in the Northern District of California. VBS initially provided hearing health benefits to clients, customers, and patients. However, during the COVID-19 pandemic, VBS started billing for COVID-19 testing.

40. According to the Provider Enrollment Chain and Ownership System (“PECOS”), VBS enrolled in Medicare around January 21, 2020, with a principal address of 39899 Balentine Drive, Suite 200, Newark, California 94560. MOORE is listed as CEO on the Medicare Participating Physician or Supplier Agreement.

CDPH INVESTIGATION

41. Individual 01, who is an examiner for CDPH, was interviewed by the Federal Agents on June 29, 2023. Individual 01 began an investigation into VBS around May 11, 2021, predicated by a complaint against VBS that the complainant’s family members were billed for COVID-19 tests when they were told by VBS that they would not get billed.

42. Individual 01 reviewed CDPH's internal database and learned that VBS did not have a State or CLIA license to test for COVID-19. Beginning on May 24, 2021, Individual 01 attempted to contact VBS via phone calls and emails in order to obtain further information regarding testing and licensing at VBS. On June 7, 2021, Individual 01 received an email from Moore in response to the above referenced inquiry. In the email, MOORE referenced Sun Clinical Laboratory's CLIA number and expressed that VBS had a "consultant agreement with Sun Clinical Laboratory to perform both PCR and Antigen Kit." Individual 01 shared with the Federal Agents that a lab cannot use another lab's CLIA license number. Furthermore, MOORE never shared with Individual 01 any form of the consultation agreement.

43. On June 7, 2021, Individual 01 spoke telephonically with MOORE, Chief Executive Officer at VBS. Individual 01 informed MOORE that if he was performing on-site COVID-19 testing that he needed to have proper licensing. Individual 01 followed up the phone conversation with an email to MOORE with the subject line "REGULATORY information-Virtual Benefits Solutions" that included references for California licensing information and a warning letter to MOORE.

44. The warning letter was a "notice to cease and desist all clinical laboratory testing" and that confirmation of successful transmission constituted proof of receipt. The letter addressed to MOORE stated the following:

- a. VBS was performing COVID-19 testing, but did not possess the licensure required pursuant to Business and Professions Code section 1241.
- b. The performance of clinical laboratory testing without the required licensure could subject MOORE to civil and criminal sanctions.
- c. To notify CDPH, in writing, within 10 days of receipt to confirm that all testing had been ceased.

45. Individual 01 closed their investigation on July 29, 2021, noting there was no further communications from VBS after the warning letter was sent and the website for the company no longer existed.

46. Nevertheless, on August 9, 2021, Individual 01 forwarded the email sent on June 7, 2021, to MOORE with the subject line “FW: REGULATORY information-Virtual Benefits Solutions.” An email read receipt from MOORE was received by Individual 01 a few minutes later. Individual 01 did not have any additional contact with MOORE.

47. On August 20, 2021, CDPH received an application for a CLIA application for certification and requested a “Certificate of Waiver”² license from VBS, which was granted a CLIA ID# 05D2245109 on December 10, 2021. The email address listed on the application was MOORE’s. MOORE signed the application as the Chief Executive Officer.

48. On his initial and revised application, MOORE listed the effective date of December 1, 2020, on the CLIA application for certification. During an interview with Individual 01 by Federal Agents, Individual 01 relayed that the effective date cannot be backdated prior to the application date. Based on my training and experience, this was an attempt to backdate the application to claim eligibility to be covered under CLIA sooner than the initial submission date of August 20, 2021.

49. MOORE listed his type of laboratory as “Mobile Laboratory.” During an interview with Individual 01 by Federal Agents, Individual 01 relayed that a mobile laboratory required special testing equipment and temperature control capabilities in which a personal vehicle did not meet. The vehicle identification number listed as the mobile laboratory was a 2020 Lincoln Aviator SUV.³

HRSA UIP BILLINGS

50. The HRSA UIP program was implemented through an online portal which was administered by UnitedHealth Group Optum. Providers requesting reimbursement were required to submit claims through the online portal by entering provider identification and billing

² A Certificate of Waiver allows the holder to perform tests that were waived by the FDA. Waived kits are kits that cannot cause serious harm to the user such as a glucose test.

³ A review of documents received during the investigation outlined a checklist for medical assistants collecting COVID-19 specimen samples to be mailed to CQuentia, which is a lab located in Texas.

information and patient information, among other things. The claims were electronically received in Minnesota and after verification, reimbursement was sent via an automated clearing house transfer which originated from the state of Utah.

51. From approximately June 6, 2020, through March 17, 2022, VBS billed approximately more than \$43,797,187 and was paid approximately more than \$21,225,338 from the UIP. The UIP stopped accepting claims for reimbursement on March 22, 2022, due to a lack of sufficient funds.

52. An analysis of the UIP claims identified that between June 8, 2021, a day after being notified to cease and desist, and December 9, 2021, a day before receiving a CLIA license number, VBS billed for more than \$4,958,384 and was paid more than \$2,048,487 for COVID-19 testing.⁴

53. On July 12, 2023, Federal Agents received a report from HHS-OIG, Division of Data Analytics, which reviewed if any VBS billed UIP patients were also enrolled in Medicare or Medicaid. Based on my training and experience, VBS cannot submit claims to be reimbursed through HRSA if an individual is enrolled in Medicare or Medicaid. An analysis of the UIP claims identified that approximately 5,437 of the patients to whom VBS provided were possibly enrolled in Medicare or Medicaid and therefore not eligible for reimbursement under the UIP program. HRSA paid VBS approximately \$4,107,884 on those claims.⁵

INTERVIEW WITH FORMER VBS EMPLOYEE

54. Individual 02 filed a hotline complaint to the HHS-OIG hotline on November 15, 2022, about VBS' improper billing methods for the UIP without checking if the patient was uninsured. Individual 02 was the director of human resources at VBS and had knowledge of VBS' business practices and was involved in meetings with MOORE.

⁴ Procedure codes for specimen collection (G2023, G2024, and 99211) were not included in the total billed and paid to VBS calculation because a CLIA waiver was not required to collect samples. COVID-19 testing codes were 86328, 87426, 87428, 87635, 87811, U0001, U0002, U0003, and U0004.

⁵ Data source July 6, 2023. First date of service was July 8, 2020, and the last date of service was March 17, 2022.

55. During an interview with Individual 02 on February 6, 2023, Individual 02 shared that VBS sent employees into the field to conduct COVID-19 tests and that tests were not done in an office. Individual 02 stated VBS rented multiple virtual offices that were not brick and mortar office locations. VBS' office address located at 39899 Balentine Drive, Suite 200, Newark, CA 94560 was a virtual office rented through Regus. A virtual office provides a business with a physical address without any physical office space. A review of some of the claims' data indicated patients were billed "in office."

56. Individual 02 shared that medical assistants who administered the COVID-19 tests were told they did not have to ask patients for insurance information. MOORE and VBS management told Individual 02 that the COVID-19 tests were essentially free to patients and VBS's involvement in UIP was above board. Individual 02 stated VBS automatically billed UIP regardless of the patient's insurance coverage.

57. Individual 02 was concerned about VBS billing for patients who did not get COVID-19 tests or were tested only once but billed for multiple tests. When Individual 02 brought the concern to VBS management Individual 02 was terminated shortly afterwards.

58. On January 31, 2023, Individual 03 was interviewed by Federal Agents.⁶ Individual 03 was hired as a medical assistant and worked from the VBS office located at 3940 Valley Avenue, Pleasanton, California 94566. Individual 03 was one of six managers in the medical support staff division and supervised three employees. During Individual 03's time at VBS, Individual 03 received complaints from other medical assistants and patients alleging VBS overcharged their insurance by billing multiple COVID-19 tests a day. Individual 03 stated MOORE often worked at the Pleasanton, California location.

59. On January 26, 2024, Federal Agents spoke again with Individual 03. Individual

⁶ Individual 03 filed a hotline complaint to HHS-OIG under a false name since there was no option to remain anonymous.

03 recalled that COVID-19 supplies were stored at the VBS location at 3940 Valley Avenue, Pleasanton, California during the time period of alleged crimes and that MOORE had an office there.

RELATOR COMPLAINT

60. A Relator Complaint against VBS was filed on October 25, 2023, in the Northern District of California. Relator 01 and Relator 02 (“Relators”) were employees at VBS within the billing department and had knowledge of VBS’ billing, policies, and procedures for COVID-19.

61. The Relators stated that VBS collected patient information prior to conducting COVID-19 tests through a form. However, VBS crossed out the insurance portion of the patient form and only asked the patient for identification without inquiring about the health insurance status of the patient.

62. The Relators noted that when patient insurance was known to VBS, they billed the UIP and also submitted a claim to the patient's private insurance. When the Relators discussed the duplicative billing, MOORE laughed and stated, “if they double pay us, that’s their problem.”

63. On January 24, 2024, Relator 01 was interviewed by Federal Agents and government attorneys. Relator 01 was also involved in a civil complaint that alleged VBS conducted improper COVID-19 billings.⁷ Relator 01 worked in the billing department and was initially hired as a remote, work from home employee, but later worked from the VBS office located at 301 Providence Road, Chapel Hill, North Carolina.

64. VBS had multiple remote employees across the United States who handled billing, but the billing teams all reported to the 301 Providence Road, Chapel Hill, North Carolina location. According to Relator 01, the VBS North Carolina location was the primary location from which COVID-19 billings occurred.

65. After a certain time, Relator 01 was transferred to the audiology billing

⁷ The civil complaint is filed under seal.

department. During that time, Relator 01 attended weekly virtual meetings with Joseph Hardeman (“Hardeman”) and other staff. It was common knowledge at VBS that Hardeman resided in South Africa. Hardeman was the audiologist at VBS and directed the billing department on which codes to bill health insurance plans. Hardeman was often seen lying down in bed during the weekly meetings. When Relator 01 told Hardeman that certain codes cannot be billed because Hardeman was in South Africa, Hardeman would suggest a different code to Relator 01 and asked if it was allowed.

66. Relator 01 also stated MOORE was in South Africa from approximately Fall 2022 to June 2023, to hire employees to perform health insurance billing for a VBS office in South Africa. Relator 01 stated MOORE discussed purchasing a ten-bedroom house in South Africa.

67. On June 7, 2023, while in South Africa, MOORE announced during a Zoom meeting that all employees in the North Carolina office and throughout the United States were furloughed. Relator 01 stated the VBS South Africa office continued to operate and receive their paychecks.

68. On April 3, 2024, Relator 02 was interviewed by Federal Agents and government attorneys. Relator 02 worked in the billing department and was the lead Covid-19 biller at the VBS North Carolina location. Relator 02, raised concerns to her manager, whose initials are R.O., that VBS billed UIP despite VBS knowing the patient’s insurance information. Her manager responded that it was the way MOORE wanted it to be done. Additionally, Relator 02 identified another manager, whose initials are M.B.

69. The Covid-19 and Audiology billing department each had their own Microsoft Teams chat. R.O. and M.B. used the chat to give directives to the team. The chat was also used to ask questions related to billing.

70. Relator 02 used Microsoft Teams to attend virtual meetings and used the chat function in Teams to communicate with colleagues. Relator 02 recalled a chat where a colleague detailed the payment process at VBS.

FORMER VBS CLIENTS

71. On January 26, 2024, Federal Agents interviewed Individual 04. Individual 04 was the Chief Operating Officer and coordinated the COVID-19 testing at their facility. Individual 04 required weekly Covid-19 testing for their non-vaccinated employees and hired VBS to conduct such testing. A contract was entered into between Individual 04, signed around September 2021, and MOORE representing VBS, who docusigned around October 2021. VBS began testing at their facilities around September 2021, with the contract being cancelled around June, 2022.

72. Around March 18, 2022, a VBS employee, with an email domain ending in @vbshealthcare.com, emailed Individual 04 indicating VBS would no longer be testing for the uninsured because the HRSA stopped funding the uninsured program. Individual 04 replied on the same day asking for a list of individuals who it affected. Around March 21, 2022, a VBS employee responded with an email containing a hyperlink “Patient Insurance Status Sisk.xlsx.” The hyperlink web address was https://vbshealthcare-my.sharepoint.com/:x/g/personal/lpettway_vbshealthcare_com/EQPg-k_-MptBnh3rKLxhMRgBsQ8aOS5I_yHsuUBqj0GqZA?e=wZJx8Q. The web address appears to be a VBS SharePoint website.

PRIVATE PAYORS

73. On December 13, 2022, Federal Agents received information from a private payor, Health Plan 01, regarding VBS and their billing practices through a request for information. The records reflected, in part, a letter from Health Plan 01 to VBS dated February 4, 2022, regarding Health Plan 01’s audit and a corrective action notice was dated April 8, 2022.

74. The February 4, 2022, letter sent from Health Plan 01 to VBS indicated that VBS billed \$17,687,175, was paid \$10,606,426 and was overpaid \$5,061,480 for the period of July 10, 2020, to November 30, 2021. The audit conducted by Health Plan 01 covered codes to include, but not limited to 99211 and G2023.

75. The corrective action notice outlined various billing methods that VBS needed to correct. One such corrective action Health Plan 01 relayed to VBS was their billing of specimen

collection (utilizing code G2023) which was identified as unsupported for separate reimbursement. Health Plan 01's claim review identified specimen collections billed with office visit coding (e.g. 99211). VBS was notified that it must discontinue billing specimen collections which are considered integral (not separately reportable) to the office visit being billed. Based on my training and experience, when a provider bills a separate and distinct service for a service already included, that is unbundling. Unbundling refers to using multiple procedure (CPT) codes for the individual parts of the procedure to increase payment.⁸

76. CMS described CPT code 99211⁹ as: "During the PHE, CMS specified that the level one E/M visit (CPT code 99211), which can ordinarily be billed only when clinical staff perform services incident to the services of the billing physician or practitioner for an established patient, can be billed when clinical staff assess a patient and collect a specimen for a COVID-19 diagnostic test for both new and established patients."

77. CMS described CPT code G2023¹⁰ as: "Independent laboratories must use one of these HCPCS codes when billing Medicare for the nominal specimen collection fee for COVID-19 testing for the duration of the PHE for the COVID-19 pandemic. These HCPCS codes are: • G2023, specimen collection for severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) (Coronavirus disease [COVID-19]), any specimen source."

78. CMS further states, "Physician offices can use CPT code 99211 when office clinical staff furnish assessment of symptoms and specimen collection incident to the billing professionals services for both new and established patients. When the specimen collection is performed as part of another service or procedure, such as a higher-level visit furnished by the

⁸ On April 20, 2022, MOORE signed an overpayment settlement with Health Plan 01. MOORE signed a document agreeing to repay Health Plan 01 \$3,057,058 for its improper billing and wired that amount to Health Plan 01 on August 30, 2022. The settlement information is to complete the narrative and is not submitted to the Court for purposes of establishing probable cause.

⁹ <https://www.cms.gov/files/document/physicians-and-other-clinicians-cms-flexibilities-fight-covid-19.pdf>

¹⁰ <https://www.cms.gov/files/document/03092020-covid-19-faqs-508.pdf>

billing practitioner, that higher level visit code should be billed and the specimen collection would not be separately payable.”

79. On October 28, 2022, Federal Agents spoke with an employee of Health Plan 02. Health Plan 02 conducted a proactive review, on or about July 2021, of VBS, being a non-CLIA licensed audiology provider billing excessive tests. Health Plan 02 learned that VBS was an Audiologist, but primarily billed COVID-19 tests. The tests related to COVID-19 codes, included 87428, 87811, U0003, U0002, 86328 and specimen collection code G2023. Health Plan 02 learned that each code was billed 440-550 times and members had up to 6 codes billed on the same date of service. No audiology service claims were identified in the data. Health Plan 02 was unable to identify VBS and their CLIA license.

80. In June of 2022, Health Plan 02 was contacted by VBS, who offered to supply a sample of previously requested Health Plan 02 patient records. Health Plan 02’s Special Investigative Unit reviewed health care plan records for their beneficiaries. Health Plan 02 identified various issues with the documents, to include, but not limited to:

- a. Documentation did not support the billed services.
- b. No diagnosis code was present in the records.
- c. No screening questions, patient assessments, vital signs, or any medicals services were documented.
- d. The credentials of the person who authored the records was unclear.
- e. The requested list of employees, with credentials, was not supplied.
- f. No laboratory requisitions were supplied with the records.
- g. It was unclear who ordered the test services and for what reason.
- h. It was unclear if the person who authored the records was in-person or virtual.
- i. The codes billed by VBS indicate an attempt to unbundle charges that would normally be inclusive in other codes billed on the same claim. There were instances where multiple codes were billed that appear to be for the same, single

service...billing G2023 and 99211 for the same encounter.

j. VBS also stated that they perform Rapid Antigen testing on site using: Carestart, CovClear and the Abbott ID Now machines. These are all at-home tests and do not require the use of any laboratory equipment to support billing the codes VBS habitually billed.

k. The VBS provided records also included a one paragraph attestation by a Medical Assistant (or unlicensed individual) that they witnessed the administration and completion of the SARS-CoV-2 Rapid Antigen Test. It would appear that the provider's only services include the observation of an at-home test taken by a Health Plan 02 beneficiary.

81. Health Plan 02's employee indicated that the service was dramatically misrepresented by the inflated codes billed on claims. Health Plan 02 identified at the time of the interview that their exposure to VBS' improper billing was approximately \$290,000 of the \$1,000,000 VBS billed.

ANALYSIS OF FINANCIAL RECORDS

82. California Secretary of State records indicate Virtual Benefit Solution Inc, Hearing Clinic was incorporated on September 5, 2013, and as of today, has seemingly been operating for at least 10 years. In March 2020, as the COVID-19 pandemic materialized, the UIP was established and made available \$1 billion to provide reimbursement to health care providers for the testing and treatment of uninsured patients.

83. Pursuant to grand jury subpoenas, Federal Agents reviewed and analyzed numerous financial records including but not limited to bank statements, deposited items, deposit slips, withdrawals, and wire instructions. Around the same time the UIP funding became available, VBS opened new bank accounts at First Republic Bank ("FRB") and Wells Fargo Bank.

84. FRB account -4193 was opened on May 21, 2020, in the name of Virtual Benefits Solutions Inc DBA Virtual Hearing Solutions with MOORE listed as the sole authorized signor.

Almost three months after FRB account -4193 was opened, the first UIP payment of \$1,046 was received on August 20, 2020. The account went on to receive approximately \$2,690,786.50 in UIP payments before the account ceased banking activity on April 29, 2021, and the remaining balance of \$278,278.32 was withdrawn and deposited into FRB account -5211.

85. FRB account -5211 in the name of Virtual Benefits Solutions Inc with MOORE listed as the sole authorized signor, was opened around the same time as the deposit of \$278,278.32¹¹ From April 2021 to around January 2023, FRB account -5211 received approximately \$18,524,901.08 in UIP payments.

86. At some point in time, Health Plan 01 identified unusual billing transactions from VBS and conducted an internal audit. That audit identified transactions from as early as July 10, 2020, through November 30, 2021, that required corrective actions. Similarly, CDPH's investigation into VBS began around May 11, 2021. CDPH determined that VBS did not have the proper licensing to operate and sent a cease-and-desist letter on June 7, 2021.

87. A former VBS employee and Relator complaint both alleged VBS did not ask for patient insurance information and did not verify if they were uninsured. Furthermore, the complainants alleged VBS knowingly submitted improper billings to the UIP.

LAUNDERING OF PROCEEDS

88. From approximately June 3, 2021, to August 16, 2021, during the time period of expected fraud by Health Plan 01, several monetary transactions over \$10,000 were conducted through VBS account -5211. Based on my conversations with Federal Agents, I know payments by check and wire transfers between or among bank accounts is considered a monetary transaction within the meaning of 18 U.S.C. § 1957.

89. On July 8, 2021, \$250,000 was debited from VBS account -5211 for check #1001 signed by MOORE and paid to Tim Ambrose. The check memo line states "Repayment of

¹¹ Subpoenaed records produced two signature cards for FRB account -5211. One is dated May 27, 2021, and the other is dated June 4, 2021, however the first bank statement transaction is April 29, 2021.

Loan.” Based on my conversations with Federal Agents and the prior account balances calculated through direct tracing practices, there is probable cause that the check debit of \$250,000, contained greater than \$10,000 in proceeds of wire fraud.

90. On July 8, 2021, \$11,250 was debited from VBS account -5211 for check #1002 signed by MOORE and paid to Tim Ambrose. The check memo line states “QT interest on Loan.” Based on my conversations with Federal Agents and the prior account balances calculated through direct tracing practices, there is probable cause that the check debit of \$11,250, contained greater than \$10,000 in proceeds of wire fraud.

91. On July 12, 2021, \$500,000 was debited from VBS account -5211 for check #1004 signed by MOORE and paid to Virtual Benefits Solutions Inc. The check memo line states “Transfer Funds for Bus.” Based on my conversations with Federal Agents and the prior account balances calculated through direct tracing practices, there is probable cause that the check debit of \$500,000, contained greater than \$10,000 in proceeds of wire fraud.

92. On August 5, 2021, \$50,000 was debited from VBS account -5211 for check #1007 signed by MOORE and paid to Eugene Adams. The check memo line states “Personal Loan.” Based on my conversations with Federal Agents and the prior account balances calculated through direct tracing practices, there is probable cause that the check debit of \$50,000, contained greater than \$10,000 in proceeds of wire fraud.

93. On August 5, 2021, \$136,453 was debited from VBS account -5211 to fund a wire transfer to Emoyo USA LLC. The originating beneficiary information on the wire transfer states “VIRTUAL BENFITS SOLUTIONS.” Based on my conversations with Federal Agents and the prior account balances calculated through direct tracing practices, there is probable cause that the wire of \$136,453, contained greater than \$10,000 in proceeds of wire fraud.

94. On August 16, 2021, \$230,000 was debited from VBS account -5211 to fund a wire transfer to Investors Title Insurance Company. The originating beneficiary information on the wire transfer states “VIRTUAL BENEFITS SOLUTIONS (BUYER) ANNA FAMILY OFFICES LLC (SELLER).” Based on my conversations with Federal Agents and the prior

account balances calculated through direct tracing practices, there is probable cause that the wire of \$230,000, contained greater than \$10,000 in proceeds of wire fraud. Subpoenaed title records indicated the \$230,000 wire to Investors Title Insurance Company on August 16, 2021, funded a money deposit to purchase real estate located at 301 Providence Road, Units 311 & 321, Chapel Hill, North Carolina. The property was purchased in the name of Virtual Benefits Solutions Inc., Hearing Clinic for a total purchase price of \$2,298,165.

95. Wells Fargo account -5550 was opened on June 5, 2020, in the name of Virtual Benefit Solutions Inc with MOORE listed as the sole authorized signor. In 2021, the account received approximately \$14,848,105 in credits funded primarily by transfers from other VBS bank accounts and check deposits from private payors including Health Plan 01. Between March 22, 2021 and April 13, 2021, approximately \$1,850,000 was transferred in numerous transactions from Wells Fargo account -5550 to Wells Fargo account -0149.

96. Wells Fargo account -0149 was opened on December 15, 2015, in the name of MOORE with MOORE listed as the sole authorized signor. On April 23, 2023, \$1,735,400 was debited from Wells Fargo account -0149 for check #1011 signed by MOORE and paid to MOORE. There is no memo line on the check. The check was deposited on April 23, 2021, in Wells Fargo account -2705.

97. Wells Fargo account -2705 was opened on March 27, 2021, in the name of MOORE with MOORE listed as the sole authorized signor. On May 24, 2021, a \$1,104,072.65 wire was sent to Old Republic Title Company with a note indicating the payment was for Escrow Number 0112020023 Down Payment.

98. Law enforcement databases indicate 152 Alamo Springs Drive, Alamo, California was sold on May 21, 2021, to MOORE for a total purchase price of \$2,674,000. The address listed on the May 2021 Wells Fargo account -2705 bank statement and the June 2021 Wells Fargo account -0149 bank statement is 43456 Ellsworth Street, Unit 3334, Fremont, California. The address listed on the June 2021 Wells Fargo account -2705 bank statement and the July 2021 Wells Fargo account -0149 bank statement changed to 152 Alamo Springs Drive, Alamo,

California.

99. The address listed on the April 2022 Wells Fargo account -5550 bank statement is 39899 Balentine Drive, Suite 200, Newark, California and the address listed on the May 2022 Wells Fargo account -5550 bank statement changed to 152 Alamo Springs Drive, Alamo, California.

100. From around June 2022 to January 2023, approximately \$1,389,405 was wired to Capitec Bank in South Africa.

101. Based on my training and experience, and conversation with FBI and IRS-CI agents, I know that individuals communicate using emails and chats to discuss business operations and plans. I know that individuals who receive emails from regulatory agencies often share those emails to conspirators and employees.

102. Based on the email correspondence between CDPH Individual 01 and MOORE, there is probable cause to believe that MOORE disregarded the regulations set by CDPH and continued to allow VBS to improperly bill the UIP for COVID-19 tests.

103. I know that individuals who share SharePoint links generally have access to various files related to business operations and plans that are shared with conspirators and employees. Based on the email correspondence between Individual 04 and VBS, there is probable cause that VBS maintained a SharePoint website which may contain files related to the business and operations that were used to communicate business operations and plans with conspirators, employees, and customers.

104. I know that individuals who use the chat and video conference functions in Microsoft Teams often discuss business operations and plans with conspirators and employees. Based on the interview with Relator 02, there is probable cause that VBS used Teams to communicate business operations and plans with conspirators and employees.

105. Further, I know most companies and individuals use their email, video and chat, and filesharing accounts for various purposes, including to track or correspond regarding policies, business operations, patient appointments, inventory status, and accounting purposes.

Further, I know that information derived from a search of a business email, video and chat service, and filesharing account is also likely to reveal the names of employees, contractors, and service providers. These types of individuals may serve as witnesses able to provide more data to law enforcement about the scope and frequency of MOORE's and VBS' suspected billing for COVID-19 test under the UIP, as well as his direct involvement in the submission of claims reimbursement without a proper federal or state license.

106. Further, I believe there is probable cause to conclude the following examples of communications will be captured in the **Subject Account**, and serve as evidence of the Target Offenses:

- a. Records and communications related to the billing and reimbursement for the COVID-19 tests under any insurance;
- b. Records related to the federal and state licensure required to test for COVID-19;
- c. Records and communications related to setting up a laboratory for COVID-19 testing;
- d. Records relating to who created, used, or communicated with the account or;
- e. Identification of other accounts, domains, IP addresses, and computers owned or controlled by the same individual(s) controlling each account;
- f. The following documents that tend to establish the identity of the person or the persons in control of the account: identification documents (such as driver's licenses or passports), photographs, bills, receipts, vehicle registration documents, statements, leasing agreements, personal address books, calendars, daily planners, and personal organizers.

CONCLUSION

107. Based on the information above, there is probable cause to believe that a search of the information described in Attachment A will reveal the items described in Attachment B,

which are evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 1347 (healthcare fraud), 371, 1349, 286 (conspiracy to commit healthcare fraud and defraud the United States), 287 (submission of false, fictitious or fraudulent claims to the United States), and 1957 (engaging in monetary transactions in property derived from specified unlawful activity). Therefore, I respectfully request that the Court issue the proposed search warrant.

/s/ *Jin Tae Kim*

Jin Tae Kim
Special Agent
HHS-OIG

Sworn to before me over the telephone and signed by me pursuant to Fed.R.Crim.P. 4.1 and 4(d) on this 9th day of July 2024.

Kandis Westmore
HONORABLE KANDIS A. WESTMORE
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with account located at vhshealthcare-my.sharepoint.com and domain vbshealthcare.com that is stored at premises controlled by MICROSOFT, a company headquartered at One Microsoft Way, Redmond, Washington.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

To ensure that agents search only account(s) described in Attachment A, this search warrant seeks authorization to permit employees of MICROSOFT (the “**Provider**”) to assist agents in the execution of the warrant. To further ensure that agents executing this warrant search only the account described as vhshealthcare-my.sharepoint.com and under the domain vhshealthcare.com for MICROSOFT SharePoint and Teams chats, videos, and messages, the following procedures will be implemented:

I. Search Procedure

The search warrant will be presented to **Provider’s** personnel, who will be directed to isolate those accounts and files described in Section II below:

- a. In order to minimize any disruption of computer service to third parties, **Provider’s** employees will create an exact duplicate of the accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;
- b. Law enforcement personnel will thereafter review the information received stored and identify and copy only the information authorized to be further copied as described in Section III below; and
- c. Law enforcement personnel will then seal the original duplicate of the accounts and files received from **Provider**, employees and will not further review the original duplicate absent an order of the Court.

In the review of information provided pursuant to this warrant by **Provider**, the government must make reasonable efforts, to the extent required by the Fourth Amendment, to use methods and procedures that will locate and expose those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant while minimizing exposure or examination of irrelevant or attorney-client privileged files to the extent reasonably practicable.

II. Files and Accounts to be Copied by Provider's Employees

To the extent that the information described in Attachment A is within the possession, custody, or control of **Provider**, regardless of whether such information is located within or outside of the United States, and including any chats, records, files, logs, or information that has been deleted but is still available to **Provider** or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **Provider** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails, SharePoint, and Teams data stored in the account from January 1, 2019, to July 1, 2023, including copies of communication or file stored on the account, draft files, the source and destination addresses associated with each file, the date and time at which each file was sent, and the size and length of each file;
- b. All records or other information regarding the identification of the account, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All subscriber records for the account;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, documents, and files;
- e. All records associated with the uploading, sending, and receipt of images, documents, and files, including all time and date stamps, device information, and IP addresses for each interaction;
- f. All records pertaining to communications between **Provider** and any person regarding the account, including contacts with support services and records of actions taken; and
- g. All records or other information regarding the user's account settings.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

III. Information to be Seized by the Government

All information described above in Section II that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 1347 (healthcare fraud), 371, 1349, 286 (conspiracy to commit healthcare fraud and defraud the United States), 287 (submission of false, fictitious or fraudulent claims to the United States), and 1957 (engaging in monetary transactions in property derived from specified unlawful activity) those violations involving VBS and MOORE and occurring after January 1, 2020, specifically, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Records or communications pertaining to public and private health care benefit programs and insurers involving COVID-19, which includes any and all items pertaining to enrollment, rules and regulations, complaints, audits and investigations, compliance, billing, claims, and policies and procedures, including but not limited to Health Resources & Services Administration ("HRSA") Uninsured Program, any communications with the HRSA Uninsured Program, UnitedHealth Group, and COVID-19 testing partners, such as laboratories, or any other related contractor for the HRSA Uninsured Program. Records related to the federal and state licensure required to test for COVID-19.

b. Records or communications about COVID-19 testing, the purchase of COVID-19 testing kits, and laboratory policies and practices including procedures or policies of any physician or healthcare worker employed or contracted by MOORE, VBS or VHS.

c. Records or communications pertaining to patient information who underwent COVID-19 testing, including insurance information, billing under the HRSA Uninsured Program, any records or communications regarding the verification of patient insurance information, patient sign-in sheets related to COVID-19 testing, Explanation of Benefit forms, and correspondence to and from patients regarding billing, and records or communications

pertaining to providing free or discounted goods or services to any potential patients receiving COVID-19 tests. This should also include any documents reflecting patients treated or tested for COVID-19, but who may not have patient files.

d. Records or communications pertaining to or reflecting the location(s) of where patients received any kind of testing or treatment related to COVID-19, whether at VBS or VHS offices or at an off-site/mobile site location. This should include any lists, contracts, or agreements between MOORE, VBS, VHS, or any physicians/healthcare workers employed or contracted by MOORE, VBS or VHS, and any other locations, or paperwork documenting locations and dates of treatment.

e. Records or communications pertaining to the marketing of, testing for, or treatment of COVID-19 by MOORE, VBS, VHS, or any physicians employed or contracted by MOORE, VBS or VHS, including policies, procedures, guidelines, instructions, guidance, presentations, off-site location services, commercials, videos, or documents that otherwise list services offered.

f. Records or communications providing VBS or VHS employees or contractors any information about how to perform their job functions, such as training manuals, provider manuals, regulations, bulletins, reports, newsletters, notices, pamphlets, handbooks, other publications, and correspondence relating to proper billing and documentation procedures and any documents regarding instructions for billing insurance providers or carriers.

g. Records or communications pertaining to billing practices, computer billing system, or any other methods of posting charges manually or otherwise, preparing invoices, making adjustments or alterations in billing, generating billing reports, or other procedural operations associated with the tracking of services rendered and billing, including account receivable journals and ledgers from.

h. Records or communications pertaining to billing and payment files reflecting billing to any insurer, including Medi-Cal, Medicare, TRI CARE, or to the HRSA Uninsured Program, including documentation batch information sent to or received by the HRSA Uninsured

Program containing information including patient rosters, batch identifiers, or any other list of patient names from.

i. Records or communications to the present pertaining to current and former employee/contractor files, including but not limited to licensed medical professionals, medical assistants, coding/billing staff, and administrative staff, such as applications for employment, employment contracts, employee and contractor work schedules, salaries and compensation, bonuses, time sheets, reference/background checks, professional certifications, training, performance evaluations, disciplinary actions/terminations, improvement plans, and payroll records.

j. Records or communications pertaining to or reflecting any businesses in which MOORE, VBS or VHS have a financial relationship with, investment stake in, ownership of, controlling interest of, or management in, including, but not limited to, contracts, articles of incorporations, shareholder agreements, offering memoranda, or memoranda of understanding.

k. Records or communications pertaining to the finances of MOORE, VBS or VHS, including but not limited to bank account records, bookkeeping records, accountant work-papers used in preparation of loan applications, and other financial statements, including income statements, income tax returns, balance sheets, general ledgers, general journals, gross receipts records, sales records, income records, cash receipts records, cash receipts schedules, disbursement records and/or journals, sales and purchase records and/or journals, accounts receivable and accounts payable records, cost of goods sold records, loan agreements, loan receivable and payable ledgers, daily sales schedules, evidence of travel expense, and all sales and expense invoices including all invoices documenting expenses paid by cash (currency) or bank check (cashier or teller checks).

l. Documentation of ownership of real property or other entities involving Virtual Benefit Solutions, Virtual Hearing Solutions, and/or Tyrone MOORE. Documentation may include deeds of trust, promissory notes, beneficiary demands, title company records, and escrow files, and lease contracts and agreements.

m. Records or communications pertaining to the purchase of and/or payments of money owned for real estate and/or vehicles or other personal living expenditures by Tyrone MOORE.

n. Items evidencing the obtaining, transfer, and/or concealment of assets and the obtaining, transfer, concealment and/or expenditure of money to include business books and records, invoices, receipts, records of real estate or securities transactions, escrow files, vehicle and vessel purchase records, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, checkbooks, loan statements, work papers, and records reflecting the purchase of assets.